DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

30 Sep 05

MEMORANDUM FOR DISTRIBUTION

Subj: INFORMATION TECHNOLOGY (IT) POLICY GUIDANCE FOR FISCAL YEAR 2006 EXPENDITURES

In Fiscal Year 2006, as in recent years, our information management/ information technology (IM/IT) efforts will focus on creation of a joint, net-centric environment that delivers knowledge dominance to Naval warfighters. To that end, we must invest only in projects that are aligned with the Department's strategic vision and aimed at our goals of a secure, interoperable architecture, providing web-enabled services and full dimensional protection. Department of the Navy (DON) activities must comply with this guidance in order to expend and/or release funds for IM/IT investments.

Application, Data and Portfolio Management

- Application Approval Required - No development, modernization, operation, or maintenance of software applications that are not designated either "Approved" or "Allowed with Restrictions" in the DON Applications and Database Management System (DADMS) by the appropriate Functional Area Manager (FAM) is authorized. All applications must be registered in DADMS and must obtain either "Approved", or "Allowed with Restrictions" (AWR) designation by the applicable FAM prior to being connected to a DON network.

- XML - To ensure interoperability across the DON and preclude the Department's being tied to a single vendor's solution, the DON Policy on the Use of Extensible Markup Language (XML) of 13 Dec 2002, posted for reference at http://www.doncio.navy.mil, prohibits use of proprietary extensions to XML-based specifications in DON IT systems.

- DON XML NDR - All Navy and Marine Corps commands developing systems using XML should apply the development guidance and standards identified in the DON XML Naming and Design Rules (DON XML NDR). Adherence is necessary to maximize interoperability and enable a net-centric environment across the Department. The DON XML NDR may be viewed at http://www.doncio.navy.mil .

ESI/SmartBUY - Commercial software agreements have been established that coordinate multiple IT investments to leverage the Federal Government's purchasing power for best-priced, standards-compliant products. These agreements are managed through the DoD Enterprise Software Initiative (ESI) and the Federal SmartBUY program. SmartBUY does not mandate use of particular brands of software, but DON activities purchasing software for which agreements have been awarded must use the SmartBUY agreements. Agreements are currently in place for ESRI, Manugistics, Novell, WinZip, ProSight and Oracle database products (Oracle database products and options must be purchased via SmartBUY. Other Oracle products may also be ordered via SmartBUY). These, and all future SmartBUY agreements will be publicized through the DoD ESI website, http://www.esi.mil. DON activities shall comply with Defense Federal Acquisition Regulation Supplement (DFARS 208.74), DODI 5000.2, "Operation of the Defense Acquisition System," paragraph E4.2.7 (links to both references at http://akss.dau.mil/jsp/default.jsp), and the USD AT&L - DoD CIO Joint Policy Memorandum dated September 16, 2003, "Department of Defense (DoD) Support for SmartBUY Initiative" (http://www.esi.mil/uploaded_documents/0924GUE45834.doc), when acquiring commercial software.

- Oracle License - A Navy-wide Oracle database enterprise license has been established through ESI/SmartBUY, providing all Navy employees ashore and afloat, including authorized support contractors, the right to use the Oracle database product. The enterprise license enables transition from older or unsupported versions of Oracle database products, and its use is mandatory where Oracle has been selected as the database solution. POC for ESI and enterprise licensing: Mr. Floyd Groce, (703) 607-5658, or floyd.groce@navy.mil .

- Microsoft Enterprise Agreement – MARADMIN 363/05 requires all Marine Corps procurements for any Microsoft software be made via Marine Corps Systems Command's enterprise contract. POC for the enterprise agreement is Ms. Teresa Hardisty, (703) 432-0270 or teresa.hardisty@usmc.mil.

Navy Server Policy

- The ASN(RDA) memorandum of November 12, 2004, "Purchase of Servers and Application Hosting Services" stipulates that no new or upgraded servers or application hosting services are to be purchased, leased or rented at any level of the Navy organization for CONUS (Continental United States) ashore use without the prior written approval of PEO-IT. The restriction extends to purchase, lease, or rental of servers or application hosting services under support contracts. Servers or application hosting for Top Secret information, compartmentalized information, and cryptologic activities related to National Security Systems are specifically excluded. The policy memorandum may be viewed at http://www.peo-it.navy.mil/SAHRAP .

Navy Policy on Registration of IM/IT Networks, Servers and Associated Network Devices

- Registration Required for Navy Activities – NAVADMIN 124/05 established the requirement for networks, servers, and associated network devices to be registered in DADMS. Additionally, it required that FAM "Approved" and "AWR" applications be linked only to registered servers and to report the termination of server applications not FAM "Approved" and/or "AWR" in DADMS. No development, modernization, operation or maintenance of unregistered networks, servers, or associated devices is authorized. In Fiscal Year 2006, a Business Case Analysis (BCA), DADMS registration, and designation as "Approved" by the Enterprise Services FAM must be completed before any network, server or associated device procurement, or block upgrades to existing networks, servers, or associated devices.

Internet Protocol Version Six (IPv6)

- All assets being developed, procured or acquired for the Global Information Grid (GIG) must be IPv6 capable and must be interoperable with IPv6 systems/capabilities. This explicitly includes all acquisitions that reached Milestone C after October 1, 2003. The current version of the

DoD Information Technology Standards Repository (DISR), viewable at http://disronline.disa.mil/VJTA/index.jsp, reflects this requirement. DoD policy on IPv6 is stated in DoD CIO memoranda of June 9, 2003 and September 29, 2003, viewable at http://ipv6.disa.mil .

Mobile Voice and Data Services

- The Department is engaged in initiatives to reduce the costs of handheld wireless communications services. The ASN(RDA) memorandum of March 7, 2005, "Department of the Navy Acquisition Policy on Mobile (Cellular) Phone and Data Equipment and Services" requires that all wireless communication support for Navy or Marine Corps activities in CONUS (Alaska and Hawaii excepted) must be obtained via the nationwide contracts awarded by Fleet Industrial Supply Activity San Diego (FISCSD) or the Navy Marine Corps Intranet (NMCI). The memorandum allowed for continuation of contracts extant at the time the policy was signed until expiration, or October 1, 2005, whichever came first. The policy does not apply to secure communications devices. Waiver authority resides with PEO-IT. Further information about the policy, a set answers to frequently asked questions; and links to ordering services, waiver request procedures and a pdf of the policy memo may be found at http://www.peo-it.navy.mil/MobilePhonePolicy .

Voice Over Internet Protocol (VOIP)

- VoIP is the current commercial preference for converged voice and data transmission. To ensure consistent architecture, standards and security across the DON enterprise, activities are directed to coordinate with the DON Deputy CIO Navy or Marine Corps, as appropriate, before employing a VoIP solution other than NMCI's.

Smart Card Technology

- The Common Access Card (CAC) is designated as the Department of Defense (DoD) primary physical and logical access badge, and carries DoD Public Key Infrastructure (PKI) credentials. Homeland Security Presidential Directive 12 (HSPD-12), signed by the President on August 27, 2004, established the requirement for a common standard for identification credentials issued by the Federal Government for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. DoD will ensure that the CAC meets HSPD-12 mandates and associated Personal Identity Verification (PIV) standards. DON activities procuring access control systems and other smart card technology must use the CAC as the primary means to gain physical and logical access. Procurement of smart card technology other than the CAC must have DON CIO review and approval and conform to the requirements established by HSPD-12. DON Smart Card-PKI policy is available on the DON CIO website at https://www.doncio.navy.mil. The PIV standard and supporting documents relative to HSPD-12 are available at http://csrc.nist.gov/piv-program. The DON CIO point of contact for other-than-CAC approval is Ms. Sonya Smith, (703)601-0081, or sonya.r.smith1.ctr@navy.mil .

- All desktop/laptop computers procured by DON activities for connection to unclassified network services/NIPRNET must include smart card readers compatible with the DoD CAC, and all commands must enable cryptographic logon as soon as the required infrastructure is in place. The ASN(RD&A) memorandum "Smart Card Requirement" of 3 June 2003 is available on the DON CIO website at https://www.doncio.navy.mil.

Information Assurance (IA) and Public Key Infrastructure/Public Key Enablement (PKI/PKE), Wireless Technology Security

- FISMA - The Federal Information Security Management Act (FISMA) applies to the Department's IA program, and requires certification and accreditation of all DON systems and networks, all-hands IA awareness training, specialized training for users with privileged network functions, oversight of system and network protection (including metrics on system and network intrusions), annual security plan and contingency plan testing, and annual security reviews and evaluations. IA funding requirements should be separately defined as IA funding, as this number itself is a reportable IA metric. POC: Mr. Jim Collins, (703) 602-6202, or james.e.collins.ctr@navy.mil.

- DITSCAP - DODI 8500.2 (DoD Information Assurance Implementation) requires that all IA and IA-enabled products acquired meet the Common Criteria National Information Assurance Partnership (NIAP) framework, per NSTISSP Policy 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products. NSA and NIST-sponsored laboratories perform certification testing, which increases product acquisition costs. If there is no Common Criteria Protection Profile for an IT-enabled product (such as a Personal Digital Assistant), the DON will apply DITSCAP to perform a similar product vetting before allowing its connection to Department networks. Resources required for writing and staffing DITSCAP packages should be factored under the total IA funding umbrella. POC: Ms. Jennifer Korenblatt (703) 602-6759, or jennifer.korenblatt.ctr@navy.mil.

- Public Key Infrastructure/Public Key Enabling (PKI/PKE) - DON IT systems must provide the capability for digital signature of email messages to ensure data integrity; encryption of email messages containing For Official Use Only (FOUO), Sensitive but Unclassified (SBU), or privacy information; certificate-based client authentication for private websites; and cryptographic log-on. POC: Mr. James Mauck (703) 601-0579, or james.mauck.ctr@navy.mil.

- Privacy - Per Section 208 of the E-Government Act of 2002, DON activities must perform privacy impact assessments (PIA) before developing or procuring IT systems that collect, maintain, or disseminate information in a personally identifiable form from or about the public. A summary of the E-Government Act, and a link to the text of the Act, may be found at http://www.whitehouse.gov/omb/egov/g-4-act.html . POC: CAPT Deborah McGhee (703) 602-6882, or deborah.mcghee@navy.mil.

- Wireless Technology Security – Wireless devices integrated with or connected to DoD networks are considered to be part of those networks, and must comply with DoD Directive 8500.1and DoD Instruction 5200.40 (DoD instructions & directives may be viewed at http://www.dtic.mil/whs/directives/index.html). Additionally, for data devices and services, strong authentication, non-repudiation, and personal identification are required for access to a DoD Information System (IS). To ensure consistency of architecture, standards, and security across the DON enterprise, commands are directed to coordinate with their respective DON Deputy CIO, Navy or Marine Corps, prior to expending resources on any infrastructure initiative involving a wireless data solution outside of the existing NMCI solution. Existing wireless installations are required to comply with security regulations and will be addressed on a case-by-case basis. POC: Ms. Patricia Christensen (703) 601-0230, or patricia.christensen@navy.mil.

- "CYBER Condition ZEBRA" - To improve overall network security posture, the Navy has embarked on a focused process in an operation titled "CYBER Condition ZEBRA". The effort will be focused upon geographic regions. First, the Untrusted Network Protection Policy (UTNPP) will be implemented, followed by isolation of legacy networks from NMCI to determine what services must be transitioned to NMCI to enable elimination of those networks. In FY06, ACNO(IT) and NNWC will commence permanent legacy network shutdown, starting with the Hampton Roads Enterprise Network. All Navy commands will develop, fund and execute transition plans for their legacy networks services to NMCI consistent with the "CYBER Condition Zebra" execution plan (the fragmentary order for "CYBER Condition ZEBRA is NETWARCOM msg. 261652Z MAY 2005).

BMMP Certification Requirement for Development & Modernization

- 10 U.S.C. 2222 (as added by Section 322 of the Ronald W. Reagan National Defense Authorization Act (NDAA) for Fiscal Year 2005) effective October 1, 2005, prohibits obligation of funds for any defense business system modernization that will have a total cost in excess of $1 million unless it is reviewed by the appropriate Office of the Secretary of Defense (OSD) Investment Review Board (IRB), certified by the designated OSD approval authority, and the certification is approved by the Defense Business System Modernization Committee (DBSMC). Accordingly, all DON activities acquiring, developing, or modifying business information technology systems that meet the statutory threshold of "defense business system modernization that will have a total cost in excess of $1 million" must follow the DON Business Information Technology System Pre-Certification Workflow Guidance, Version 1.6.5 (downloadable from http://www.doncio.navy.mil) to obtain IRB review and certification, and DBSMC approval prior to obligating any funds for such modernization. 10 U.S.C. 2222 (a link to the text is provided at http://www.doncio.navy.mil/(yvlefm45yu1bqtejp52wrdbu)/contentview.aspx?ID=1639&ShowMore=true) specifically provides that obligation of funds for a defense business system modernization that has a total cost in excess of $1 million without an approved certification is a violation of the Anti-deficiency Act, 31U.S.C.1341(a)(1). The DON Pre-Certification Guidance establishes the Department's process to obtain pre-certification per Department of Defense implementing guidance for all Tier 1, 2 and 3 Defense Business System Modernizations. POC for BMMP certification questions is Mr. Bob Wagner, (703) 607-5671, or robert.m.wagner.ctr@navy.mil

The following information is provided as notice of policy that will be implemented in the near future that may affect your IT planning:

- The Office of the Secretary of Defense employs the DOD IT Registry to maintain an IT inventory, including National Security Systems (NSS), in compliance with Congressional requirements, and to serve as a technical repository supporting various assessments. The DON IT Registry is uploaded to the DoD IT Registry. All Mission Critical (MC), Mission Essential (ME) and Mission Support (MS) information systems, including NSS, must be registered in the DON IT Registry by 30 September 2006, and no FY07 funds may be expended on any MC, ME or MS DON IT systems, including NSS, that have not been registered in the DON IT Registry (or its expected FY06 successor database, the DoD IT Portfolio Repository (DITPR)). POC for IT registries is Mr. Jeff Greene, (703) 602-6845, or jeffrey.greene1.ctr@navy.mil.

Questions concerning the guidance above, or the Department's business process transformation efforts may be directed to Barbara Hoffman, DON CIO Investment & Performance Management Team Lead, at (703) 602-6847, or barbara.hoffman@navy.mil.

D. M. Wennergren

Distribution:
CNO (N09B, N098)
CMC (DCMS, C4)
CHNAVPERS
COMLANTFLT
COMPACFLT
COMNAVEUR
COMUSNAVCENT
COMSC
COMNAVRESFORCOM
COMNAVMETOCOM
COMNAVSECGRU
COMNAVNETWARCOM
BUMED
COMNAVAIRSYSCOM
COMSPAWARSYSCOM
COMNAVFACENGCOM
COMNAVSUPSYSCOM
COMNAVSEASYSCOM
ONI
NETC
NAVSTKAIRWARCEN
DIRSSP
COMNAVSPECWARCOM
NCTSI
COMOPTEVFOR
COMNAVSYSMGTACT

Copy to:
Immediate Office of the Secretary (ASN(M&RA), ASN(I&E), ASN(RD&A), ASN(FM&C) (FMO)
(FMB-B)
GC
CNO (N82)